6. SECURITY

6.1 INTRODUCTION

This section is intended to raise awareness of the potential truck-related security concerns facing the District, and to present successful security practices from American and European cities. The section concludes with a series of recommendations to District officials for actions to raise the level of security against truck-borne threats.

In contrast to an individual facility, an entire urbanized area cannot be 100 percent secured against the threat of a vehicle-borne improvised explosive device (VBIED). Governments must always balance enhancing security with enabling the free flow of goods vital to the local and national economies. In its post-September 11th report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, the National Academy of Sciences cites five characteristics of transportation systems that factor into any effort to increase transport security:

- Openness and accessibility
- Extent and ubiquity
- Emphasis on efficiency and competitiveness
- Diversity of owners operators, users, and overseers
- Entwinement in society and the global economy

Constraints on a comprehensive truck security strategy in the District include the following:

- Truck transport is vital to the economy of the District, even though its economy is much less dependent on the movement of goods than other major metropolitan areas.
- Truck security in urban areas is generally oriented toward the protection of individual structures or campuses by the implementation of standoff zones and access control procedures. A comprehensive policy would identify an outer perimeter surrounding sensitive facilities within which special truck control measures are implemented routinely or during times of heightened threat.
- Truck security requires coordination among agencies concerned with highways and roads, public safety, and emergency management in the District and its two neighboring states. Within the District, the Federal Government fields 32 distinct law enforcement agencies.
- Security stakeholder organizations experience tension between sharing security information with, and withholding it from security partners. This is especially true for the many Federal agencies having security responsibilities within the District.
- Security technology and physical barriers notwithstanding, security is only as effective as the people and procedures surrounding the technology and enforcing the barriers. Training, simulations, and continual testing are expensive and necessary.

Countermeasures against terrorist acts do not only include defending against an attack in progress, but also forestalling an attack before it begins and mitigating terrorism's tragic and costly effects afterwards. Table 10 indicates the complete range of countermeasures needed to protect sensitive facilities and urban infrastructure against truck-borne threats. In

the table the countermeasures are arrayed against the timeline of events before, during, and after a terrorist attack.

This study gives the outlines of a truck security policy focused on large trucks (weighing over 10,000 pounds) and buses. The measures discussed in this section will emphasize deterrence and detection with some attention to prevention and defense. There are two key issues that overarch the discussion in the balance of this chapter concerning the implementation of a systematic solution to truck-borne threats focused on large trucks in the District:

- The District government, in general, and DDOT, in particular, controls only a part of the system. The Federal Government exerts enormous power and, depending on the agency, may or may not consult with the District regarding truck security.
- Clearly, the threat from VBIEDs is not confined to, or even projected to principally arise from, the large trucks and buses that are the subject of this study. However, these vehicles—especially hazardous materials tankers—are not only highly visible to the public, but offer the opportunity to leverage safety, credentialing, and operational technology being installed in large trucks for multiple purposes, including security.

Table 10. Security Countermeasures and Their Relevance to DDOT

Timing	Countermeasure Category	Description	DDOT Truck Security Relevance
Pre-attack	Preparedness (Design)	Measures such as personnel training, creation of policies and procedures, design of streetscapes, truck routes, truck inspection stations	Interact with other city, regional, and Federal agencies
	Prevention (Intelligence, Surveillance, and Interdiction)	Activities to prevent the launching of a terrorist attack	Use oversight of motor vehicle traffic to uncover pre-attack terrorist planning activities
	Deterrence	Countermeasures which are visible to potential attackers and which deter an attack by raising the risk of apprehension or lowering the probability of success	Use oversight of commercial motor vehicle traffic to help deter potential attackers

Timing	Countermeasure Category	Description	DDOT Truck Security Relevance
During attack	Detection	Activities to detect an attack that is underway	Use oversight of commercial motor vehicle traffic to help detect attackers; use special purpose equipment to detect explosives and weapons of mass destruction (WMD)
	Defense (Protection)	Activities to delay or prevent an attack in progress, and to protect and harden facilities against attack	Interact with agencies protecting facilities-at-risk, agencies planning for hardened streetscape features, and law enforcement agencies having truck-interdiction capability; direct truck traffic flow away from facilities-at-risk
	Mitigation	Activities to reduce the deleterious effects of an actuated attack	N/A
Post-attack	Response	All actions by authorities in response to a terrorist act	Invoke existing emergency management plans
	Recovery	All activities needed to return the affected area to normal after an event; may also include activities for investigation and attribution	Invoke existing recovery plans

6.2 THE TRUCK-BORNE THREAT IN THE DISTRICT

6.2.1 Characterization of the Threat

The extent of the terrorist threat to the District is obvious. The threat is clearly not confined to trucks, but security experts regard trucks as a highly likely means of delivering destruction in an attack. Potential targets could include:

- Federal agencies
- Federal monuments and landmarks
- Embassies
- Military facilities
- District critical infrastructure
- Financial, religious, cultural, and patriotic icons
- Venues of gathered crowds

Terrorist scenarios involving large trucks and buses may involve a vehicle operated by either a trusted driver (where the terrorist device has been surreptitiously loaded onto or attached to the vehicle) or by a terrorist (where the vehicle has been obtained through legitimate or illegitimate means). The vehicle itself, such as a hazardous materials tanker, may be the means of destruction, or a VBIED may be present. In addition, the VBIED could be a means of dispersing chemical, radiological, or biological agents.

In one sense, the threat from large trucks in the District may be more manageable than in other large metropolitan areas. Because of its role as the nation's Capital, the District has proportionately fewer workers involved in industries related to the movement of goods than the United States as a whole. In addition, there are a reported 19 routes suitable for large trucks to enter or leave the city. Rock Creek, and the Potomac and Anacostia Rivers, surround the core area of the city on three sides. The fourth side, however, is connected by numerous streets to towns in Maryland. The overall threat from terrorism in the District is large and the probability of attackers' using large trucks cannot be discounted.

6.2.2 Hazardous Materials Trucking

One source of public concern is hazardous materials transportation. Because of the risk hazardous materials transport presents, Volpe queried District agencies that monitor or otherwise oversee this traffic or its shippers. Under Federal hazardous materials transportation law,[10] hazardous materials transport in the United States is governed by regulations that define the requirements for:

- hazardous materials carrier registration[11]
- placards and packaging[12]
- restrictions on unnecessary transport through tunnels, over bridges, or through heavily populated areas[13]
- restrictions on the transport of highly dangerous materials, such as explosives and fissionable nuclear materials[14]
- detailed and stringent limits on the ability of state and local governments to restrict hazardous materials transport routing without Federal preemption[15]

In the aftermath of September 11th, the U.S. DOT promulgated new and proposed regulations to increase the control and oversight of hazardous materials shipments. These measures include:

- security plans to be written by hazardous materials carriers (new)[16]
- background checks required for a CDL hazardous materials endorsement (new)[17]
- hazardous materials carrier safety permit to be issued by the FMCSA (proposed)[18]

---

[10] 49 USC §§ 5101-5127
[11] 49 CFR Parts 171-180
[12] ibid.
[13] 49 CFR Part 397.67
[14] 10 CFR Part 71.5; 49 CFR Part 173
[15] 49 CFR Part 397
[16] 49 CFR Part 172 Subpart I
[17] 49 CFR Parts 383 and 384

- hazardous materials on-the-road telephone check-in by drivers to be required (proposed)[19]
- hazardous materials carrier technology demonstrations funded to track and protect shipments (ongoing)

Beyond participating in Federally funded programs to perform safety and hazardous materials inspections and in accordance with Federal regulations, Washington, DC area state and local government agencies do not monitor or regulate most hazardous materials transport trips. Therefore, it is difficult to quantify the volume of total hazardous materials traffic in the District.

Potential sources of threat in the District include terminal locations for hazardous materials. The most prevalent destinations for hazardous cargo in the District are gas stations. The Department of Health (DOH) Underground Storage Tank Division maintains up-to-date records on the location of underground tanks storing petroleum products used for energy production (except for residential storage of small quantities of home heating oil). The relative sparseness of gas stations within the core of the District suggests that fuel deliveries to those stations might be restricted and monitored.

Although there are no major hazardous materials shippers in the District, the District is the principal place of business for 52 hazardous materials motor carriers registered as such with the U.S. DOT Research and Special Programs Administration (RSPA) and reported in FMCSA data. Companies having hazardous materials storage or transshipment sites tend to be in the fuel oil industry.

Figure 18 indicates the current designated hazardous cargo routes in the District. These routes include Interstate 395 (excluding the 3rd Street tunnel), Interstate 295, the Southeast Freeway, and DC-295 (the Anacostia Freeway and Kenilworth Avenue).

The DOH notes that there are no true transporters of hazardous waste in the District. Officials downplayed the volume of the materials they regulate and questioned whether a legitimate shipment diverted for terrorist purposes would be of sufficient size to cause mass casualties. Hazardous materials shipped within the District are often lead-tinged hazardous waste being disposed of by a major utility company, or radioactive materials used in medical procedures.

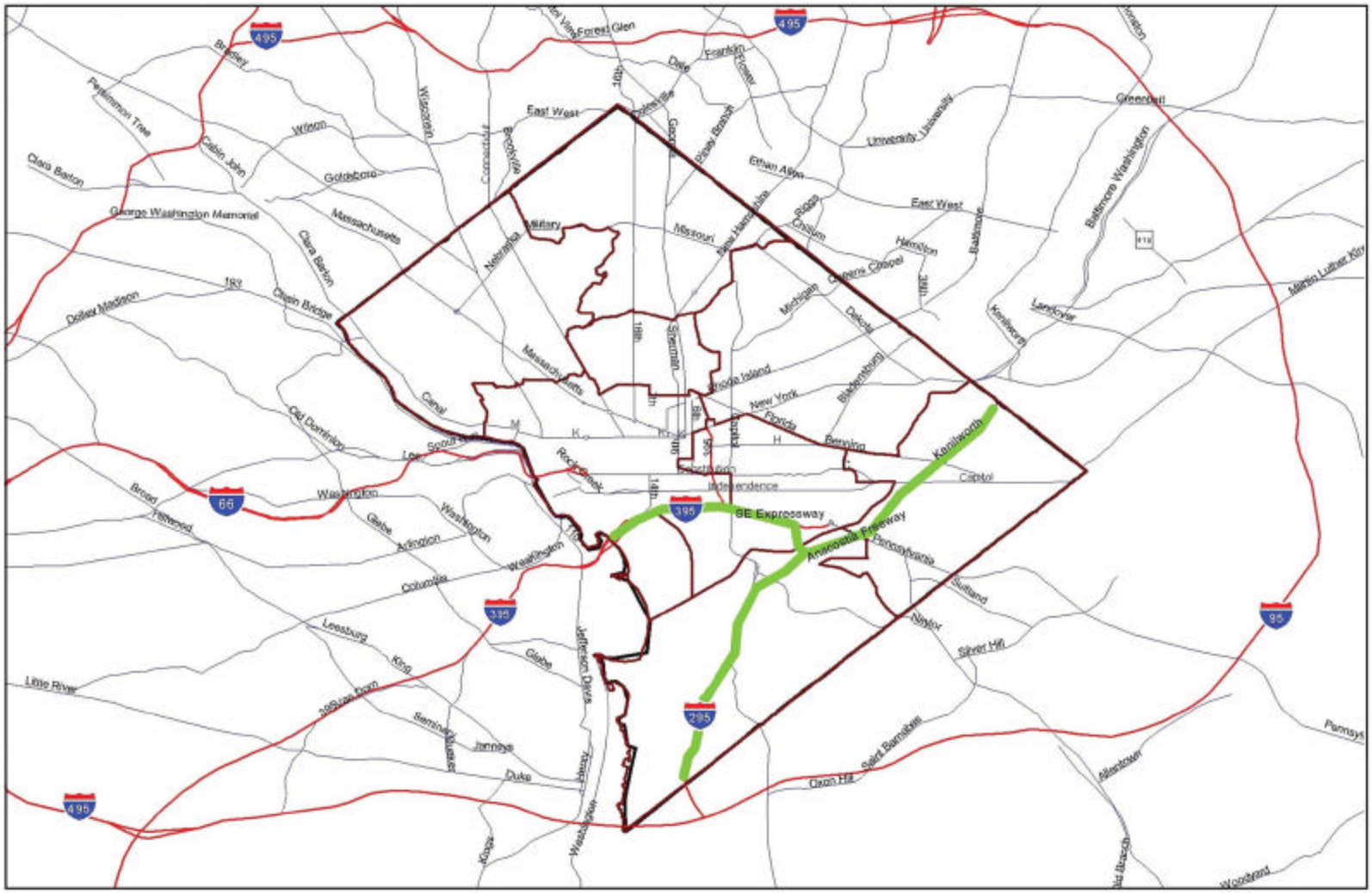
Hospitals are also the source and destination of radiological materials. The DOH has determined that the quantities and types of radioactive materials involved are not likely to pose a major public health threat. Facilities shipping and storing fissionable materials must register with the U.S. Nuclear Regulatory Commission. All shipments of radioactive materials are closely regulated and monitored. More dangerous fissionable materials are not usually shipped by truck.

---

[18] FR Doc. 03-49737

[19] 67 FR 46622; 68 FR 13250

Figure 18. Hazardous Cargo Routes in Washington, DC



The District's DCRA and the Fire and Emergency Medical Services (FEMS) Department issue permits for shipments of explosives and for their detonation. The MPD escorts high-risk explosives shipments. The overwhelming majority of these shipments are related to construction activity, fireworks displays, and movie productions. The number of explosives shipments (and detonations) is low and tends to be correlated with construction activity. However, the MPD expressed concern about the not-so-rare incidence of unplacarded trucks carrying hazardous materials in the District.

Continuing analysis of the geo-locational relationships of sensitive facilities and the likely routes of truck-borne threats, including the location of terminals for hazardous materials, will be necessary to reconcile truck security countermeasures with the changing cityscape. The ability of the analysis (and the countermeasures) to accommodate change rapidly is advisable even in an urban area that is as institutionally stable as the District.

6.3 TRUCK SECURITY STAKEHOLDERS IN THE CAPITAL REGION

Creating a series of policies, countermeasures, and responses oriented toward increased security against truck-borne threats requires the participation and leadership of agencies concerned with:

- truck traffic management and truck safety
- hazardous materials storage and transport monitoring
- security and law enforcement.

Multiple District agencies having responsibility for multiple policy areas must be brought together to address truck security, policies, and countermeasures. At the same time, responses need to bridge jurisdictional boundaries across the Washington, DC metropolitan area as well. The elements for a terrorist attack will be assembled from resources imported into the District. If these elements can be interdicted before entering the District, the chances of preventing an attack will be increased.

The number of stakeholders involved in truck security is large and diffuse ranging from Federal security agencies to relatively small units of the DOH. In addition, the impact of any policies implemented will fall on the private sector. Therefore, Volpe has sought input from private sector organizations, District agencies outside of DDOT, neighboring state agencies, the Federal agency concerned with truck and bus safety, and Federal law enforcement and security agencies. Many of these agencies were contacted as part of the larger comprehensive truck management agenda, but security concerns were discussed in many of the "best practices" interviews.

The overall picture that emerges is one of divided responsibilities, even among Federal agencies. The tasks before all of these agencies are large and their resources are limited. With the creation of the DHS, the organizational home of key Federal security agencies has changed. Because of the security concerns, many agencies were not willing to divulge the details of their strategies; however, the general outlines of their concerns will be summarized while maintaining anonymity.

6.3.1 District Agencies

There are a number of District agencies that have incidental or tangential concerns with truck security. These agencies collect data that can be used in planning countermeasures and responses to truck-borne terrorist attacks. In addition, these agencies implement procedures that may be integrated with security-related measures that DDOT might consider. Aside from DDOT, the most salient District agencies for truck security are the MPD, the Emergency Management Agency, and the set of agencies (discussed above) that monitor hazardous materials.

The MPD is the agency that "owns" the District government's security concerns with its Domestic Security Office as the focal point. In addition, the Department's Special Services Unit Motor Carrier Unit is responsible for motor carrier safety and works with the District of Columbia Division of the FMCSA to perform safety inspections on commercial vehicles. The Department is the only District government agency outside of DDOT that receives U.S. DOT funds. As previously described, the Department also monitors and escorts dangerous cargoes. The MPD already encompasses both trucking regulation and security in its organization.

During the period of heightened alert following September 11, the Department increased the volume of its random stops of commercial vehicles. To be able to use the information on trucking patterns accumulated from these stops, the MPD created a motor carrier database for the information collected in these stops. The database contains over 27,000 records and has been shared with neighboring jurisdictions to determine if there have been any patterns of suspicious activities. Additional resources for the Motor Carrier Unit would enhance the ability of the District to notice anomalous truck operations that might indicate terrorist activity.

The MPD has built a Joint Operations Command Center, which is used during emergencies to coordinate and exchange information between the MPD and agents of the FBI and the U.S. Secret Service. Video images from MPD cameras, as well as DDOT traffic cameras are displayed in the command center.

The EMA is the lead agency for coordinating the District's response to all types of emergencies. In addition, the agency has the mandate to reduce the hazards, including terrorist threats, which the District faces. Although the agency has focused on creating emergency response plans defining the activities and responsibilities of District government departments during an emergency, as a key agency that performs liaison duties with the DHS, the EMA must be included in the planning for deterrence and prevention, as well as for response.

The agencies within the District that have some responsibility for monitoring hazardous materials provide a resource for locating the source and destination of hazardous materials from their records. These locations can be mapped to analyze possible threats and vulnerabilities. As noted earlier, the agencies with oversight for various aspects of hazardous materials are:

- DCRA
- DOH Environmental Health Administration, Bureau of Hazardous Materials and Toxic Substances
    - Underground Storage Tank Division
    - Hazardous Waste Division
- DOH Environmental Health Administration, Bureau of Food, Drug and Radiation Protection, Radiation Protection Division
- FEMS
- MPD

6.3.2 Federal Law Enforcement Agencies

The Federal Government is the major player on security issues in the District, with some agencies having wide authority to affect policy decisions normally reserved to local authorities, such as street closures around sensitive facilities. A major characteristic of Federal security-related policies within the District is that there is not just one agency with responsibilities for protecting Federal facilities in Washington, DC. The District must forge coordinating security policies with 32 independent Federal law enforcement agencies. Among the most significant are:

- U.S. Capitol Police
- DHS
    - Federal Protective Service
    - Office of National Capitol Region Coordination
    - Transportation Security Administration
    - U.S. Secret Service
- U.S. Department of the Interior, NPS, and NPS Police
- U.S. Department of State, Bureau of Diplomatic Security, Domestic Facilities Protection

Each of these agencies formulates security policies for the facilities it protects. The key to facility protection is the standoff zone within which only inspected, trusted vehicles are allowed. For the highest profile locations, state-of-the-art technology and techniques, such as the Itemizer™ detector for trace explosives, and stout physical barriers (some retractable) are used to establish a perimeter, demarcate a standoff zone, check trucks and cargo, and verify the identity of drivers.

At the same time, the architectural design of many sensitive Federal office buildings in the District does not permit separation of these facilities from the streetscape. Security officials at one facility recognized that closing off all streets surrounding the facility was infeasible given the needs of District traffic circulation, although from a facility protection standpoint such a shutdown is desirable. Even without street closure, parking adjacent to sensitive facilities is likely to be banned. Federal officials cited official coordination and working relationships with the MPD, DPW, and DDOT.

The U.S. Capitol Police has instituted among the most far-reaching policies for truck security. These include a no-truck security zone around the Capitol, a program to pre-

qualify drivers and carriers allowed to be screened for entry into the security zone, and an off-site screening facility where cargo is off-loaded, inspected, reloaded, and tagged. The screened trucks are given a time window within which the delivery must be completed.

Under a priority voiced by the Chief of the MPD, the District Council has passed a resolution allowing the MPD to enter into cooperative agreements with Federal law enforcement agencies. These agreements allow Federal law enforcement personnel to enforce District law on District streets and sidewalks surrounding Federal buildings and land. Each agreement is tailored to the needs of the signatory agencies. These agreements have the potential of forming the basis of more coordinated policies between the District and the Federal Government for the purposes of security against truck-borne threats.

6.3.3 Federal Transportation Safety Agencies

The agencies within the U.S. Department of Transportation that are charged with improving the safety of commercial vehicle operations in the U.S. include the:

- Federal Motor Carrier Safety Administration (FMCSA)
- Research and Special Programs Administration (RSPA), Office of Hazardous Materials Safety (OHMS)

The FMCSA operates the Motor Carrier Safety Assistance Program (MCSAP), which provides funds to the states for driver/vehicle roadside inspections, traffic enforcement, compliance reviews, public education and awareness, and data collection. The inspections and reviews identify unsafe motor carrier operations and are governed by the Federal Motor Carrier Safety Regulations (FMCSRs). Under MCSAP the FMCSA provides funds to the District for the MPD's Motor Carrier Unit.

The FMCSA has also underwritten a multi-agency effort led by DDOT to explore the application of Intelligent Transportation Systems (ITS) technology to trucking safety and operations in the District. The portion of ITS concerned with trucks is named Commercial Vehicle Operations (CVO). Under this initiative the Science Applications International Corporation (SAIC) is preparing the *District of Columbia ITS/CVO Business Plan* (currently in draft), subtitled "Using Technology to Maximize Highway Safety and Improve Government and Industry Productivity."

ITS refers to the application of digital and telecommunications technology to highways and vehicles so that real-time information delivered by the system helps improve traffic conditions, congestion, safety, and driver comfort. Increasingly common applications are dynamic message signs and electronic toll collection. CVO focuses on technologies such as electronic credentials, and the tracking of commercial vehicles with global positioning systems (GPS). FMCSA recognizes the potential for ITS/CVO to serve security purposes concomitantly with its primary safety mission.

OHMS issues the Hazardous Materials Regulations (HMRs) as well as procedural and registration regulations concerning hazardous materials. Many of the regulations concerning hazardous materials have been outlined earlier in this section in the discussion on hazardous materials trucking in the District. The FMCSA has the responsibility for enforcing the

HMRs in addition to the FMCSRs. The FMCSA also regulates the highway routing of hazardous materials.

6.3.4 Regional Agencies

Regional planning agencies are at the forefront of preparing analyses and are beginning to implement policies to improve the security posture of the Capital region. Relevant agencies include:

- NCPC
- MWCOG
- Capital Wireless Integrated Network (CapWIN)

The NCPC has prepared a plan that outlines the elements of security-aware streetscape design that does not detract from the esthetic essentials of Washington's institutional and monumental character.[20] The Commission has established design guidelines and principles to ensure a uniform approach to physical security features that might be proposed by the Federal Government.[21] Examples of these features might include the placement of security barriers, such as hardened lampposts, benches, and tree enclosures to form barriers between facilities-at-risk and vehicle threats. The plan delineates design zones that have been reproduced in Figure 19. While the NCPC zones were designated based on design characteristics within the zone rather than explicit security or congestion considerations, the set of zones defined by the NCPC is roughly equivalent to the "restricted zone" discussed in Section 7 of this report since the zones encompass the most congested area of the city and its most attractive terrorists targets.

The MWCOG Truck Safety Task Force published a truck safety technology analysis in October 2003. The report recommends the installation of several technologies, some of which are directly relevant to security concerns. These technologies will be discussed later in this section.

Led by the State of Maryland, the CapWIN project provides integrated wireless communications links among public safety agency personnel responding to emergencies. CapWIN integrates data and messaging systems among multistate, inter-jurisdictional transportation and public safety agencies. CapWIN, "provides a 'communication bridge' allowing mobile access to multiple criminal justice, transportation, and hazardous material data sources."[22]

6.3.5 Neighboring State Agencies

The neighboring states of Maryland and Virginia were contacted to determine their initiatives with respect to truck security, any regional coordination activities in which they

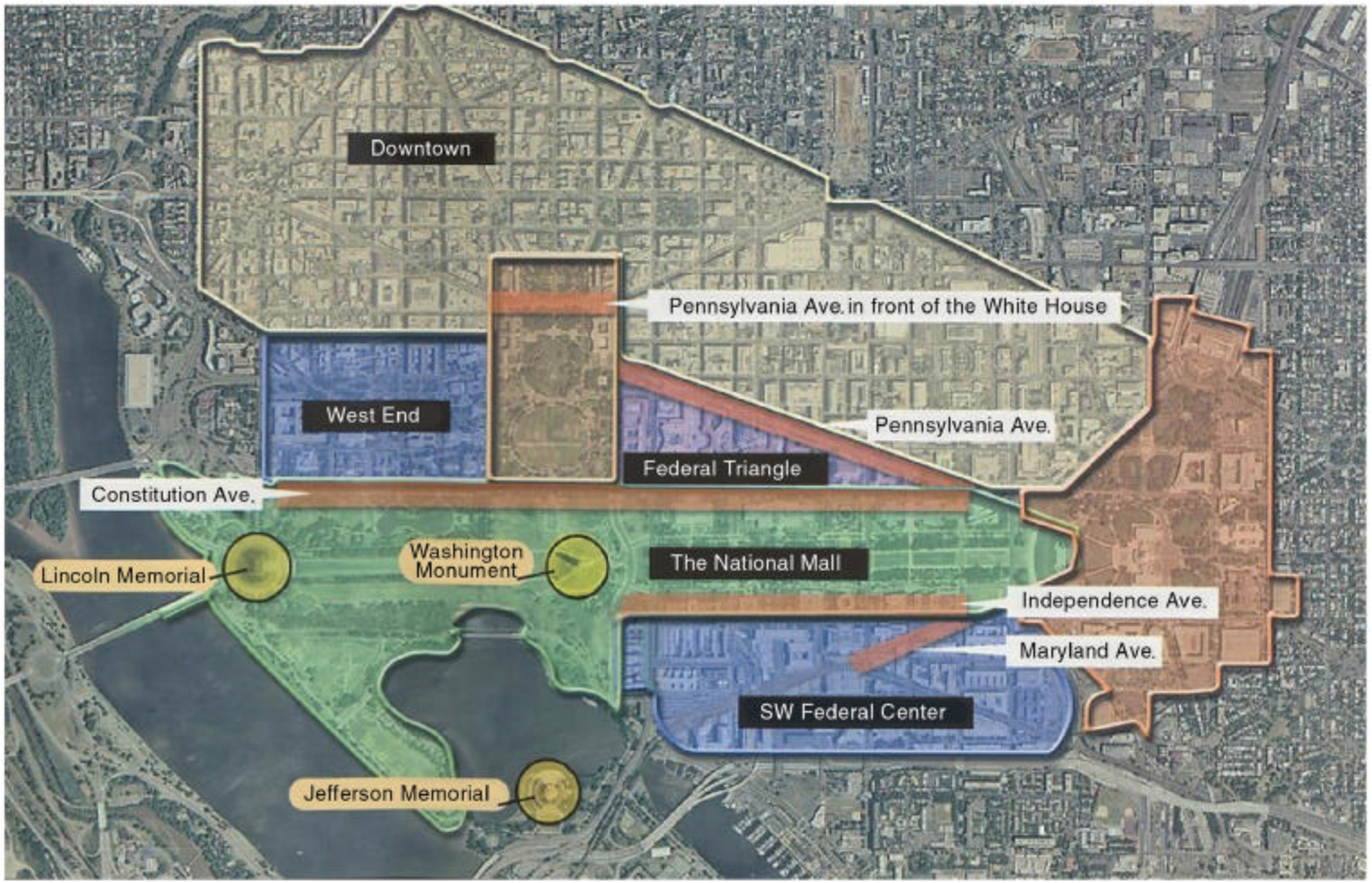
---

[20] National Capital Planning Commission. *The National Capital Urban Design and Security Plan*. October 2002

[21] NCPC, ibid

[22] See www.capwin.org

Figure 19. NCPC Contextual Zones



Source: *The National Capital Urban Design and Security Plan*, NCPC, October 2002

participated, and their policies regarding hazardous materials transport. Volpe interviewed state police and environmental agencies from each state.

The Maryland State Police reported that they instituted special measures for trucking enforcement in the period immediately following September 11th. Personnel were diverted to the Washington and Baltimore areas. In the metropolitan areas, weigh stations were opened 24 hours a day and roadside inspections were staggered, so that truckers would not be able to discern a time pattern for enforcement. Additionally, the Maryland State Police changed the proportions of the types of inspections. By reducing the number of Level 1 inspections, which require an inspector to go under the truck, the Maryland State Police were able to increase the number of trucks scrutinized. These measures will be implemented at any time the threat level is raised to orange.

The Virginia State Police also posted extra patrols in their critical metropolitan areas: Washington, DC, and Hampton Roads. Their units were particularly attentive to hazardous materials shipments. When asked about coordinating efforts, aside from the Washington, DC, regional activities reported above, the Virginia respondent mentioned a multistate committee of motor vehicle enforcement and DMVs including Maryland, Virginia, North Carolina, and West Virginia. The District does not participate in this committee.

The Maryland Department of the Environment and the Virginia Department of Environmental Quality were asked about their stance on hazardous materials transport. Both states, as required by law, implement Federal regulations with respect to hazardous materials transport. Virginia has no state-specific regulation. Maryland restricts hazardous materials traffic in the state and thus requires some additional monitoring beyond that required by the Federal Government.

6.3.6 Private Sector Companies

Trucking, bus, and package delivery companies and their respective trade organizations are aware of the potential for terrorist misuse of their vehicles. This is especially true for hazardous materials carriers. Motor carrier trade organizations and trade journals are disseminating voluntary policies that industry managers may follow to reduce the likelihood of an incident, and indeed, reduce the incidence of everyday criminal activity such as hijackings.

Hazardous materials carriers are cooperating with the FMCSA in a series of demonstrations of technological applications that enhance the safety and security of these sensitive shipments. Another public/private initiative is Operation Respond, which provides emergency responders with real-time motor carrier shipment data in the event of incidents involving hazardous materials through the Operation Respond Emergency Information System.

Package delivery companies are affected by the heightened awareness of security by their customers and they are, of course, concerned with safeguarding their drivers. While their delivery trucks are usually smaller than the large trucks under consideration in this document, their omnipresence and access to all parts of the city mean that policies

concerning these operations should be not be ignored. There is a significant threat posed by the potential for the timely delivery of coordinated shipments of improvised explosive devices. In addition, the cargo that the delivery trucks carry is delivered to staging facilities with heavy trucks. These companies have implemented national package screening programs and have cooperated with customers who request that drivers serving highly secure facilities undergo Federal Bureau of Investigation (FBI) background checks. All delivery trucks are subject to the search and inspection procedures required by secure facilities, such as the White House or the Department of State, with the time for the inspection added to the guaranteed delivery time.

In summary, stakeholder concerns include the following:

- District Government
  - Determining the priority of technology-based truck security given limited resources.
  - Developing practical prevention and preparedness policies for the DHS levels of threat when there are only two threat levels that the DHS has used short of an actual attack in progress.
- Motor Carrier Enforcement
  - Additional training in the interaction between motor carrier safety enforcement and security concerns.
  - Additional motor carrier enforcement resources are needed to implement security measures.
  - Difficulty in recruiting and retaining police with expertise in motor carrier issues.
- Private Industry
  - Added time and expense for deliveries due to security-related closures.
  - Security plans seemingly devised without input from local business community.
  - Desire of industry to understand how they would be notified of evacuation routes in the case of a major attack or other disaster, so that they can inform their drivers.
- Federal Government
  - Coordination and cooperation with the District concerning street closures around Federal facilities.
  - Adherence to the FMCSRs and HMRs regarding state and local restrictions on and monitoring of truck traffic

6.4 COMMERCIAL VEHICLE SECURITY PRACTICES OUTSIDE OF THE DISTRICT

Many valuable lessons can be learned in the area of truck security by the procedures the DHS uses at U.S. land border ports of entry. The Bureau of Customs and Border Protection (BCBP) uses various methods to try to ensure that dangerous conveyances are not allowed to enter the United States. The BCBP combines intelligence to try to target high-risk vehicles as well as random checks to ensure that low-risk categories of vehicles remain low risk. They also use technologies such as Vehicle and Cargo Inspection System (VACIS™) x-ray equipment and dogs to try to detect contraband. Figure 20 is an illustration of a mobile implementation of this technology.

Figure 20. Mobile VACIS™ Deployment at the U.S. Border

For decades, the U.S. Customs Service was tasked with ensuring that illegal contraband was not permitted to enter the United States. Their approach to this problem was simple: Limit the number of entry points into the United States, then target the highest risk vehicles for inspection. This approach was acceptable for narcotics and other illegal substances, where it was sufficient that a certain percentage was interdicted. However, when the WMD threat emerged, it was no longer acceptable that any of these weapons pass through without detection. Additional technologies have been employed to help with this effort, and more resources have been applied toward improving the intelligence that will lead to suspect shipments. Now that the Customs Service has moved to the DHS, interdicting WMD is this agency's primary focus.

Of course, the land borders of the United States are very different environments from major metropolitan areas such as Washington, DC. For instance, land borders have a limited number of well-identified entry points. Vehicles wishing to enter the United States must cross the border at one of these points and then be inspected by a DHS officer. However, there are many different roads leading into the District. To establish an effective perimeter around part or the entire city, it would be necessary to prohibit commercial vehicles from using most secondary roads and then apply the resources necessary to enforce these restrictions. While there is technology that can support such an effort, it would probably be necessary to close some roads to all traffic in order to make this scenario viable. The U.S. Capitol Police's efforts to limit vehicular traffic on Capitol Hill to only authorized and inspected vehicles illustrates the difficulty in implementing a secure perimeter. Should other areas of the District be identified as high risk for a truck bomb attack, similar procedures would need to be put in place to secure them as well.

Assuming a secure perimeter can be established around parts or the entire District, techniques used by BCBP could then be applied. Commercial vehicles would need to be screened at selected entry points and a process for inspection would be established. Depending on the level of threat, a certain percentage of vehicle inspections would be conducted at a particular degree of thoroughness. Factors such as weight, motor carrier, and manifest anomalies would be considered in targeting which vehicles would be inspected.

BCBP uses other techniques to ensure that the screening process is effective. Periodically, they will perform what is known as a "block blitz," which involves performing a thorough inspection of all vehicles in the queue at a random point in time. This provides protection against smugglers who, while monitoring the inspection process, may have identified an inspector who is not being as thorough as the others. Smugglers often target certain inspectors when they feel they have the best chance of evading detection and will purposely wait in this line. For this reason, inspectors are often rotated to different locations throughout the day.

At the land border, there is a constant need to balance security with throughput. The only way the area inside the perimeter could be 100 percent secure would be to prohibit all traffic from entering. Since this is not possible in large areas, a certain degree of risk will need to be accepted. Efforts to lower this risk through more thorough and complete inspections will result in more delays for those in transit.

The BCBP has used other techniques to make the inspection process more efficient. For example, a program of trusted carriers could be established, whereby trucking companies take it upon themselves to ensure the security of their cargo, bypassing the perimeter inspection process in most cases. The Customs Service launched a pilot program as part of the North American Free Trade Agreement that tried the trusted carrier model, and the Customs-Trade Partnership Against Terrorism uses a similar model for cargo container shipments. Since the carriers have a vested interest in being able to pass through inspection quickly and to have their facilities and vehicles secured, they are usually willing to adhere to a series of security requirements that are ultimately aimed at ensuring the safe transportation of freight from end to end.

6.4.1 Security Practices in Other Cities

All major cities face terrorist threats. The 1995 bombing in Oklahoma City shows that attacks are not limited to large cities. Examples of truck security measures in U.S. and foreign cities illustrate the extent to which security concerns are weighed in conjunction with traffic management issues. The overall truck management "best practices" interviews produced some information on truck security strategies.

London, England

The premier example is the central core of London, England. After a series of Irish Republican Army terrorist attacks in 1992 and 1993, the city of London installed a security cordon consisting of surveillance cameras and heightened police patrols. This cordon came to be known as the Ring of Steel, where the license plates of all vehicles entering the ring were vetted against a watch list of plates related to known or suspected terrorists. In 2003,

London instituted a congestion pricing strategy where all cars within the central core are charged a fee. Compliance with the charges is enforced by cameras similar to those used in airports or ports, which interface with software that automatically identifies and records the license plates of all vehicles in the core with a 90 percent rate of accuracy. Even with the wide acceptance by the public of the use of surveillance cameras in Great Britain for crime prevention, a controversy has arisen over the use of the congestion pricing cameras for general anti-crime, anti-terrorist surveillance purposes.

Baltimore, Maryland

The Port of Baltimore sponsors an interagency task force, which has created security measures. When the city is on the highest level of security alert, the State of Maryland requires truck inspections at the major southwest gateway into the city along Interstate 95. At such times, truck traffic is not allowed to leave the highway to enter the city after inspection.

New York, New York

In the immediate aftermath of September 11, all traffic into lower Manhattan was restricted. Once these restrictions were loosened, truck traffic was subject to inspection before entering Manhattan. The MPO noted that each transportation and law enforcement agency in the tri-state area had its own plans and policies for security. The MPO, in a post-September-11th safety and security report, determined that the major vulnerabilities involved the region's bridges and tunnels. The individual jurisdictions are sensitive to having the MPO take a lead role in coordinating security strategies in the region.

San Francisco, California

The DHS identified the Golden Gate Bridge as one of America's most vulnerable landmarks. It also serves as a critical element of transportation infrastructure for the Bay Area, connecting San Francisco with Marin County. Despite the fact that the bridge is considered to be a potential target for terrorism, no formal process of inspecting or screening cars or trucks has been instituted. Additional police officers have been hired to provide a show of force, and the Coast Guard monitors vessel activity beneath it, but it is acknowledged that the costs and traffic impacts associated with attempting to prevent a truck-borne weapon from being driven onto the bridge are simply too great.

6.5 TRUCK MANAGEMENT TECHNOLOGY AND SECURITY

The many technologies available to increase trucking safety, increase trucking operational efficiency, enhance highway traffic operations, and increase highway safety are being tested, deployed, and improved constantly. With increases in processing speed and decreases in the cost of data storage, technological functionality (e.g., cell phone Internet capabilities) that was not possible five years ago is now nearly universally available. Devices that may be used to increase security against truck-borne threats are now under development, and will be available within a relatively short time frame. The events of September 11 accelerated efforts to leverage these technologies for improved security of the transportation infrastructure and against vehicle-borne threats.

The broad classes of technology that are applicable to truck management and security include:

- Sensors, such as explosives detection
- Wireless communications
- Video surveillance and imaging
- Data mining and advanced data processing
- GIS and geo-locational analysis
- GPS
- Electronic driver, vehicle, and cargo identification

The FMCSA is conducting a Hazardous Materials Safety and Security Field Operational Test to measure the effectiveness of ITS safety and security technologies for safeguarding hazardous materials being transported by trucks. The test will include 100 trucks equipped with a variety of existing technologies. The technologies will be packaged in several different cost tiers, and will be tested across four different transportation scenarios. The project will test the capabilities of technologies such as:

- Driver verification using password logins, fingerprint biometrics, and smart cards
- Vehicle and load tracking using satellites and other wireless systems
- Off-route and stolen vehicle alerts using geo-fencing
- Cargo tampering alerts using electronic seals
- Driver distress alerts using driver panic buttons
- Remote vehicle-disabling in instances of known terrorist attacks

As Federal agencies institute demonstration programs among motor carriers and jurisdictions, the District should consider participating in these programs as a way to receive additional funds to test the application of advanced technologies. For example, the District could work with RSPA, FMCSA, and DHS to investigate whether options exist for applying some of the technologies listed above to hazardous materials carriers operating in the District. In addition, the District should monitor these demonstration projects and provide input into any resulting Federal regulations on the types of technologies that should be required when hazardous materials motor carriers operate in areas like the District.

The following MWCOG Truck Safety Task Force District technology recommendations have a direct application to security:

- Geo-fencing
- Panic and/or vehicle disabling systems
- Virtual weigh stations
- Infrared cameras
- X-Ray devices
- Commercial vehicle radiological systems
- Transportation worker identification cards (biometric identification)

An integrated technological strategy for truck security is based on wireless communications technologies and digital data processing. When implementing these systems, intense attention must be paid to issues of cyber security, lest digital or communications tampering

A Sample of Applicable Technologies

- *Automated Vehicle Location (AVL) and Geo-Fencing*
  Geo-fencing refers to the use of AVL technology based on GPS. Signals reporting the location of the vehicle are received at a base operations center. The center has software that compares the location of the vehicle against demarcated areas. If the vehicle crosses into a prohibited area, an alarm may be generated at the base or another location. The efficacy of GPS can be reduced if line-of-sight communications cannot be maintained with three of the satellites that determine location. However, GPS can be combined with cellular or other wireless technology to provide geo-locational information in urban canyons or other problematic locations. Geo-fencing technology is useful for identifying trusted vehicles and tracking sensitive cargoes; however, the technology is likely to be absent from or disabled on a vehicle seeking to evade controls.
- *Mobile and Relocatable Systems for Cargo Imaging or Explosives Detection*
  Several manufacturers use diverse technologies to detect the presence of contraband in truck trailers and other vehicles by creating images of the vehicle's contents. These technologies no longer need to be installed in fixed locations, but can be installed in a vehicle that can operate from changing locations or while in motion. One such system is Mobile VACIS™, which uses gamma rays to examine vehicle content. The system does not require the use of specialized protective enclosures and can scan a moving vehicle in 10 seconds. Another system is the Mobile Vehicle Explosive Detection System, which can automatically detect explosives in stopped vehicles. In the urban environment, such equipment represents a relatively unobtrusive means of detecting threats. The MPD and Federal law enforcement agencies in the District are seeking to acquire or have acquired such equipment for operational tests.
- *Video Surveillance, including infrared detection*
  Video surveillance, including infrared detection and imaging, is a means of identifying and tracking vehicles. No additional equipment needs to be installed on-board the vehicle. Video surveillance is no longer dependent on humans to monitor video images for anomalous or suspicious activity, but is increasingly linked to software that provides automated intelligence to monitor the images. The simplest applications are widely deployed license plate readers that can automatically check registration numbers against a watch list. Other systems include facial recognition, motion detection, and detection of more complex anomalous events. Not all of these products are ready for mass deployment in an urban area, but many systems are available for testing and demonstration purposes. Automated software video monitoring would provide the ability to track vehicles that are attempting to evade official countermeasures on marked truck and hazardous cargo routes.
- *ITS-CVO Automatic Vehicle Identification (AVI)*
  AVI, combined with a wireless communications mechanism like dedicated short-range communications, can also be used to track and identify trusted vehicles in an urban area. As larger numbers of trucking companies equip their trucks with this technology for interacting with the FMCSA, District officials would be able to identify most large trucks crossing the District line using the major truck routes.

render the system ineffective. The following text box provides descriptions of a sample of applicable technologies.

6.6 CHALLENGES TO IMPLEMENTING A TRUCK SECURITY STRATEGY

The policies, countermeasures, and responses needed to address truck-borne threats touch upon the responsibilities of multiple agencies in multiple jurisdictions. The effectiveness of these measures will have a direct bearing on the safety of the District's residents and labor force, including the highest officials of the nation. There are several challenges to implementing a comprehensive truck security strategy that addresses the entirety of the District's urban space.

- *Who is in charge of implementing a truck security strategy for the District?*
  More specifically, is DDOT the appropriate agency? Security is a function of police agencies. However, with respect to transportation, public safety officials, including the police, focus on the resources that are required for emergency preparedness and response—evacuation routes, maintenance of infrastructure functionality in case of widespread power failure, and deployment of resources in the event of an attack. The MPD is underfunded for their present responsibilities, even without asking the department for increased attention to truck-based terrorism. Given that the MPD has other priorities, DDOT can provide the leadership in bringing the relevant agencies together to forge a truck security strategy that is integrated with overall truck monitoring and controls. However, as the programs are developed, the MPD will be the lead agency for implementing these efforts and for working with Federal law enforcement agencies.

- *What is the relationship of Federal law enforcement agencies to the District with respect to a truck security strategy?*
  Federal law enforcement agencies, most notably the U.S. Secret Service, have the authority to close streets and restrict traffic (and have exercised it) without prior consultation with the District government. Overarching security concerns will necessarily limit the extent that the Federal agencies communicate their plans for the most serious emergencies. However, from the standpoint of planning for preparedness, prevention, deterrence and detection during what has come to be the "normal" state of alert, these agencies can coordinate with the District government to ensure that commerce within the District remains viable and to enable District government resources to be a first line of defense outside of the core area containing key Federal facilities. Different Federal law enforcement agencies have practiced varying levels of coordination with the District concerning the effects of their security policies on traffic.

  The MPD Joint Operations Command Center is a model for cooperation between Federal and District law enforcement agencies. Implementation of a comprehensive truck security strategy will require a similar level of coordination.

- *What is the role of technology in truck security and do its benefits justify the resources necessary for implementation, operation, and maintenance?*

The continued incorporation and increasing ubiquity of what is broadly called technology in all areas of economic activity is an expected feature of modern life. Competitive pressures, cheaper devices, and Federal regulatory incentives are leading trucking companies to increasingly install technology to improve their operational efficiency in serving their customers and in interacting with government agencies. Some of these technologies can be leveraged to serve the purposes of truck security, especially as they become more widespread.

6.7 THE AVAILABLE RANGE OF STRATEGIES

The strategies available to DDOT fall in the following general areas:

- Integrate truck security measures with truck tracking and control mechanisms for other purposes, especially ITS/CVO.
- Aggressively pursue all opportunities to coordinate security measures with other District, Federal, regional, and neighboring state agencies.
- Become the lead agency for demonstrations and tests of advanced technology related to truck security in the District.
- Institute truck screening and inspection, especially for hazardous materials shipments.
- Implement a systemic, layered series of countermeasures.

6.7.1 Integrate Security with ITS/CVO and Crime Prevention

Many security measures can be integrated with other ITS/CVO and crime prevention measures. Any new projects or implementation enhancements in these areas should be evaluated against security requirements. A small increment of resources may enable the ITS or crime prevention installation to serve the needs of security.

The use of ITS is rapidly spreading. While the experience of the British shows that the redirection of ITS resources for security purposes is likely to be controversial, ITS planners are rapidly increasing the capabilities of ITS installations to be useful for security purposes.

A draft *ITS/CVO Business Plan* has been produced by SAIC and is being reviewed by the sponsoring agencies. The plan recognizes that CVO and security are complementary. It proposes several projects that are directly relevant to security concerns. Although later versions of this document may present a different set of specific projects, proposals in the current draft include a hazardous material vehicle monitoring system and an electronic fencing project.

With respect to anti-crime measures, the District has already installed closed-circuit televisions for the prevention of criminal and terrorist acts. Extensions of this system may be useful in identifying commercial motor vehicles, particularly those that are being operated in a suspicious way. Research is continuing in linking video surveillance with facial recognition software, but recent tests have been unsuccessful.

6.7.2 Coordinate with Intra- and Extra-Jurisdictional Agencies

District officials noted that an effective response to issues of truck-borne threats would need to start at the Capital Beltway in Maryland and Virginia. This will necessitate coordination with law enforcement and transportation agencies in the affected areas of these states.

6.7.3 Lead Technology Demonstrations

As the Nation's capital, the District is in a unique position to be on the cutting edge of using technology and stringent truck control policies to implement a security strategy. In addition to the FMCSA program, the DHS is beginning to implement port security demonstrations. Although not a port, the District might seek to design a demonstration project that shows how similar technologies can be used in the urban setting. The District can work with Federal agencies to become a test bed for policy and technological applications for security.

6.7.4 Screen Trucks, Especially Hazardous Materials Haulers

If a decision were made to restrict commercial vehicle traffic from an area of Washington, DC, a "trusted carrier" concept could be established for those wishing to provide transportation inside a secure perimeter. Carriers would need to screen their own cargo and maintain a secure storage/transfer facility outside the perimeter.

There are two ways to implement a secure perimeter. One is similar to the method the U.S. Capitol Police employs and involves establishing a pre-screening area for all non-trusted commercial vehicles and monitoring them as they move from the screening facility to the perimeter. The other method involves allowing only trusted or government-owned vehicles inside the perimeter, and off-loading all deliverable material from other carriers at an external transfer facility. Obviously, both of these alternatives have significant negative impacts in terms of cost and on the economic vitality of the businesses inside the secure perimeter. Just-in-time delivery of production materials, perishable goods, and general inventory has become a requirement for businesses wishing to remain on a level playing field in a competitive environment. The likelihood of a terrorist attack using a truck-borne weapon would have to be extremely high to warrant establishing a large secure perimeter.

In the current threat environment, it is more practical to consider smaller, more manageable perimeters such as those established around the White House and U.S. Capitol. Locations that also rank high on the list of potential terrorist targets might need to be similarly isolated, especially if the threat level were to increase. Precisely how these perimeters should be set up and operated needs to be outlined in a security plan that considers the areas of responsibility for the Federal and District governments, various safety and law enforcement officials, and employees of the businesses and agencies inside the perimeter.

DDOT should develop a truck security plan that describes actions that are to be taken during periods of high terrorist threat. This plan should identify key areas that need to be protected, and the actions needed to establish a secure perimeter. The DHS can provide a prioritized list of facilities and structures as guidance, but in general, these would be places that are icons of the Federal Government, key pieces of transportation infrastructure, and locations where large numbers of civilians may be located. The security plan should focus on ways to

make these areas more difficult to attack, and concepts for efficiently maintaining this security posture long term, should a high threat of terrorism become more protracted.

Routes approved for the conveyance of hazardous materials should be reconsidered given their potential for use as terrorist weapons. These routes should ensure safe standoff distance from areas that are high on the prioritized list of critical assets, and signs should be erected so that the routes are clearly marked.

As discussed in Section, Federal regulations place strict requirements on state and local governments with respect to restrictions on interstate truck traffic. Any screening of hazardous materials haulers could only be implemented with the agreement of the U.S. DOT.

6.7.5 Define Truck Security Zones

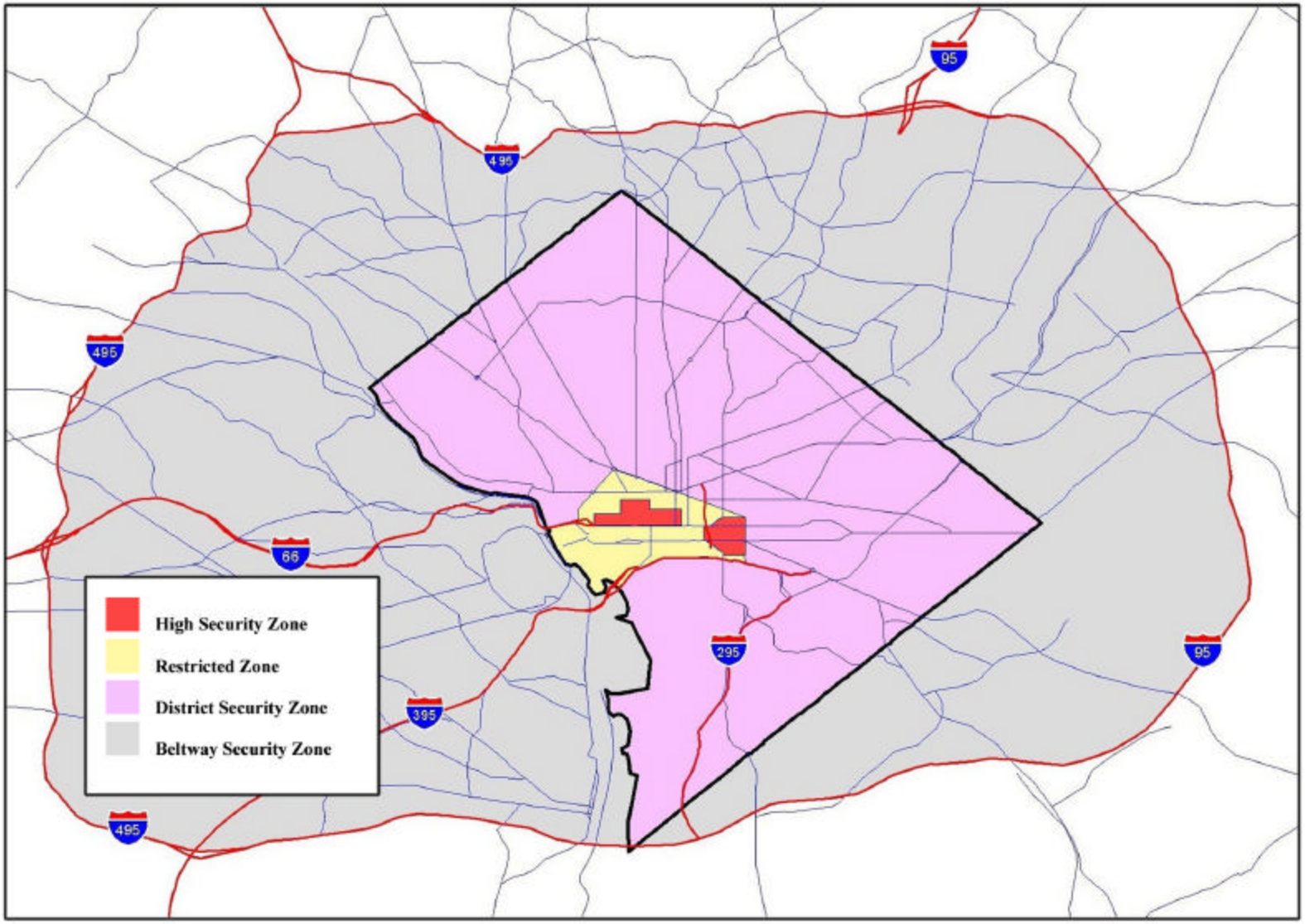
The kinds of measures suggested above, including creating a perimeter and instituting screening procedures, require the delineation of areas in the Washington, DC, region where a range of such measures can be applied. The zones, when first designated, can be used as a framework around which specific plans for truck security are drawn.

In coordination with Federal authorities and neighboring states, the District government can create a series of roughly concentric security zones surrounding the National Mall, the White House, and the Capitol Building. Over time, layered countermeasures and responses can be structured, with restrictions and other countermeasures based on the vulnerability and importance of potential targets within the zone. Zones closer to the National Mall area would have the strictest security measures and would require the closest coordination with Federal security agencies, while those farther out could have progressively more lenient measures in times of lesser threat, but at the same time would be the location of a series of detection (and possible interdiction) capabilities that could intercept a threat before it reached the inner zones.

Figure 21 shows the proposed zones, centered on the most secure red zone (actually two noncontiguous areas—one centered on the White House and the other on the U.S. Capitol), and continuing outward with the yellow, purple, and gray zones. The zones could be used to design a gradient of security measures as a truck moved from the Beltway toward the core of the District.

Starting from the Capital Beltway, the gray zone extends to the District line and is, of course, under the jurisdictions of Maryland and Virginia. Effective coordination, including policies of information sharing, and complementary procedures during periods of especially heightened threat are needed, as well as additional resources devoted to increased routine monitoring of truck traffic within the Beltway. The purple zone is bounded by the District line and the truck restriction zone defined in this study. District authorities can implement automated monitoring and geo-fencing measures close to the District line along the principal truck routes defined in this study. The yellow zone is equivalent to the restricted truck zone defined earlier in this document. Truck traffic would be permitted in this zone during daytime hours only under permit. The red zone comprises two areas: one includes

Figure 21. Proposed Washington, DC Regional Truck Security Zones



the White House, and key agencies such as the FBI and the State Department; the other roughly coincides with the U.S. Capitol no-truck zone.

Table 11 outlines the characteristics of the truck security zones. The attributes described are meant to be suggestive of the kinds of countermeasures to be instituted in each zone given the security threat level and the degree to which Federal, Maryland, Virginia, and District officials have control, particularly during times of heightened threat. Technology is a key to the countermeasures in all but the gray zone. The idea of technology portals in the purple zone is briefly described below. Even in the gray zone, technology is likely to be important, but the deployment of resources will be prioritized by the Maryland and Virginia state governments. The ERP refers to the emergency response plan that would be activated in the case of attack**.**

Table 11. Draft Characteristics of District Truck Security Zones

	Law Enforcement Agencies	District Technology Applicable?	Fuel Deliveries to Gas Stations	Threat Level		
				Yellow	Orange	Red
Red Zone	Federal, MPD	Yes	Prohibition considered	Screening; Detection; Identification	Screening; Detection; Identification	Traffic ban ERP
Yellow Zone	Federal, MPD	Yes	Restricted delivery	Truck restrictions	Truck restrictions; Detection Identification	Traffic ban ERP
Purple Zone	MPD	Yes	No restrictions	Focused inspections; Technology portals	Focused inspections; Technology portals	Screening ERP
Gray Zone	MD, VA police	No	No restrictions	Normal inspections	Focused inspections	ERP

6.7.6 Evaluate and Implement Countermeasures by Attack Phase

Broadly speaking, if all countermeasures were implemented, trusted trucks and buses operated by trusted drivers carrying verified cargo would be (1) continuously inspected for surreptitious improvised explosive devices, and (2) only travel at times and along routes known to the authorities. Alternate routes would be equipped with surveillance cameras to monitor the streets for unauthorized trucks and buses. In addition, all such vehicles would be equipped with foolproof remote engine kill switches with other means available to law enforcement agencies available to stop a suspicious vehicle.

Short of a war on U.S. shores, no municipality—not even Washington, DC—is likely to implement the full range of countermeasures for all trucks and buses. However, it is necessary to evaluate the efficacy of implementing subsets of these measures depending on

the type of commercial vehicle and the level of threat declared by the DHS. A comprehensive DDOT truck security plan will consider countermeasures applicable to all pre-attack phases attack timeline.

Preparedness.
To improve preparedness, agencies can use geospatial data to determine and refine truck security policy by analyzing existing truck routes, existing truck volume (by size and type of truck), hazardous materials terminals, facilities-at-risk, and facility standoff zones. This analysis will aid in defining the truck security measures to be taken in each security zone.

Prevention.
To prevent terrorist activities, commercial vehicle drivers and the public should be educated to recognize suspicious activity. One example of such a program is the American Trucking Associations' (ATA) Highway Watch program, which is a state-by-state effort where truck drivers report incidents of all types to a single-purpose telephone line. Drivers are trained to recognize the kinds of suspicious activity that might indicate a security threat. Additionally, the ATA runs the Trucking Information and Analysis Center to be an interface with the Federal Government, principally the DHS National Infrastructure Protection Center.

Further, hazardous materials and other commercial motor vehicle drivers should be trained to inspect vehicles for explosive devices. The ATA and bus trade groups have instituted voluntary programs to raise driver awareness of the need to thoroughly inspect their vehicles and safeguard their loads. Although beyond the scope of an urban area with a lower level of goods production and movement than most urban areas, technologies exist to assist the driver in safeguarding his or her load. This countermeasure is related to the FMCSA demonstration program. Once the technology is shown to be feasible and cost-effective, the District should consider entering into a demonstration where all trucks bearing hazardous materials would be required to have some of the technologies being tested. The District could also consider requiring tour bus and long distance bus operators in the District to adhere to a minimal set of standards for training drivers and implementing anti-terrorism policies, such as bag matching for intercity trips.

Deterrence and detection.
For deterrence and detection, perimeter(s) within which truck traffic is restricted and/or monitored can be established. This countermeasure is included here as part of systematic range of options that are available to the District. New York City, London, and the closing of Pennsylvania Avenue provide examples of the implementation of perimeters. Questions still remain on to how to best integrate the measures installed as part of the perimeter and how to apply the principles of facilities protection to the establishment of a perimeter around the core area of a city.

Within the perimeter, a range of strategies is available to define its characteristics, including:

- Conduct security-aware truck safety inspections
- Restrict truck access by route, permitted times, size of vehicle
- Identify vehicle, driver, contents

- Screen truck, driver, contents
- Detect explosive, nuclear, chemical, biological materials
- Detect unauthorized intruder vehicles
- Intercept and penalize unauthorized intruder vehicles

Again, technology exists to implement these countermeasures. Last year an unnamed European anti-terrorism police agency purchased a high-tech mobile vehicle explosive detection system, where vehicles equipped with detectors can unobtrusively scan suspicious vehicles for the presence of explosives inside another vehicle. California's DOT implemented a $20 million wireless surveillance system to transmit data from seven bridges and three tunnels in the San Francisco Bay area to a command center in Oakland. These examples suggest that truck security applications could consist of the following elements:

- Use of smart cameras to detect trucks in locations where they should be absent
- Use of mobile explosive detection equipment to scan trucks
- Use of wireless technology

Defense.

Any security area must be able to defend itself against unauthorized intruder vehicles that continue operating despite restrictions or orders to stop. Defense countermeasures are likely to be in the province of law enforcement; however, communications between transportation agencies are critical to mitigate any casualties or damages as a result of the incident.

6.8 Recommendations

1. ***Appoint a lead official within DDOT to coordinate the District's integration of large truck security with the District's truck management initiative, in general, and its ITS/CVO program, in particular***. The lead may be within the proposed Motor Carrier Office. This official will work closely with the MPD (and other agencies) to implement a series of layered countermeasures. The Security Officer should have sufficient seniority to interact and influence senior officials throughout the District government and within Federal agencies.

2. ***Create a technology portal demonstration, similar to the port and borders demonstrations, using resources from FMCSA, ITS Joint Program Office, and Transportation Security Administration***. An initial focus can be to create a virtual technology portal where trucks entering the District on the Georgia Avenue NW, Pennsylvania Avenue SE, New York Avenue NE corridors could be screened for proper credentials and for explosives or radioactive materials. The kinds of technologies included could be those being proposed in the District's *ITS/CVO Business Plan.* Figure 23 shows the approximate location of the technology portals. Some scanning for radioactive materials occurs at present; however, this effort would be analogous to the kinds of scanning currently being implemented at U.S. ports. Technology offers the opportunity to scan traffic without necessarily stopping it. This would only be a first step in creating a comprehensive strategy, as methods would need to be put in place to identify and intercept evaders.

3. ***Establish truck security zones to aid planning and to define the layers of countermeasures and responses to be deployed.*** As discussed above, the establishment of truck security zones will be an aid to defining the roles of the many security stakeholders, the policies to be implemented given distance from the District core and the threat level, and the kinds of technologies that are appropriate for deployment (or testing) depending on location within the District. The measures instituted for the truck security zones (especially the red and yellow zones) may include security inspection sites, increased random security inspections, and trusted driver/carrier programs. Any such efforts would need to fall within the requirements of Federal requirements for interstate trucking.

4. ***Explore restricting the transport of gasoline tankers into the yellow and red zones.*** There are a small number of gas stations located within the core security area of the yellow zone. Because of the sensitive nature of the targets in this area, the District should consider prohibiting gas tankers from entering the area. Alternatively, a strictly enforced policy of nighttime-only deliveries can be instituted. Federal hazardous materials regulations strictly define the process state and local governments must follow to place any limits on hazardous materials trucking. Any restriction of gasoline tankers by the District would require agreement by the Federal Government, which has ruled against such restrictions in the past.[23]

5. ***Consider countermeasures, such as a unified truck inspection facility or a "trusted" carrier program, as part of a comprehensive truck security strategy within the red or yellow zones.*** Trucking, package delivery, construction and service delivery firms face a patchwork of security requirements depending on the customer being served. While it will not likely be possible for DDOT, Federal security agencies, and private property managers to institute blanket truck security procedures for an extensive portion of the red and yellow zones, DDOT should begin to explore with its Federal and private security partners the feasibility of unifying and sharing countermeasures for some subset of facilities within these zones.

6. ***Consult with Federal hazardous materials transport regulators on the feasibility of further restricting through-truck-traffic carrying hazardous materials within the District***. As in Recommendation 4, any local restrictions on hazardous materials movement are governed by Federal regulations.[24] The volume of hazardous materials through-truck traffic in the District is small by most observations, an argument that can be used both for and against pursuing a total restriction. The singular nature of the District as the Nation's Capital is an argument for consultation with Federal officials on feasible actions for further restricting hazardous materials transport in the District.

7. ***Enhance District regulations regarding the transport of hazardous materials.*** At present, only a few specific types of hazardous materials require permits to be transported within the city. Further, the procedures that carriers must undergo to obtain the permits are not well publicized. The District government should implement a

[23] 49 CFR Part 397 Subpart C
[24] ibid.

program for more closely permitting and monitoring hazardous material transport. Again, any such programs must follow Federal hazardous materials regulations governing state and local action in this area, in particular, any permitting and fee program must be "fair and used for a purpose related to transporting hazardous material, including enforcement and planning, developing and maintaining a capability for emergency response."[25]

8. ***Prepare a comprehensive truck security plan.*** DDOT will assemble data, deliberate with Federal agencies, coordinate its efforts with other District and neighboring state agencies in order to determine the feasibility of and execute the recommendations above. The results of these deliberations should be compiled into a comprehensive truck security plan that integrates individual projects into a whole. The plan should evolve over time as specific projects, such as the technology portals, are implemented and evaluated.

[25] 49 CFR 107.202

Figure 22. Technology Portals